Claims

What is claimed is:

1. A method of securing security data stored on a computer system comprising the steps of:

providing a data key to the computer system;

transforming the security data with the data key in a reversible fashion to produce encoded secure data such that the data key is required in order to perform a reverse transform and extract the security data from the encoded secure data; and,

storing the encoded secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the data key and the user authorization process in combination, provide access to the security data and such that the stored data within the computer system is encoded.

2. A method of securing security data stored on a computer system according to claim 1, wherein a same security data is encoded with several different data keys to provide several different encoded secure data such that a combination of user authorization and any of a plurality of data keys allows for retrieval and decoding.

3. A method of securing security data stored on a computer system according to claim 1, wherein a same security data is encoded with several different data keys to provide several different encoded secure data and wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of a plurality of data keys allows for retrieval and decoding.

4. A method of securing security data stored on a computer system according to claim 1, wherein the user authorization process is a biometric information verification process.

5. A method of securing security data stored on a computer system according to claim 1, wherein the data keys include a password.

6. A method of securing security data stored on a computer system comprising the steps of:

providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source; and for, in dependence upon a comparison result pairing biometric information source with a first individual identity;

providing a data key associated with a second individual identity; the data key being other than stored on the computer system;

retrieving encoded security data associated with the biometric information, and using the key data for decoding the encoded security data.

7. A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system.

8. A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for allowing access of the data to the identified individual.

9. A method of securing security data stored on a computer system according to claim 6, wherein the step of accepting biometric information source comprises imaging the biometric information source using a contact imager.

10. A method of securing security data stored on a computer system according to claim 9, wherein the contact imager is a fingerprint imager.

11. A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing a password.

12. A method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing information stored on a smart card.

13. A method of securing data comprising the steps of:

providing a first information sample to a computer system;

encoding key data in dependence upon the first information sample to produce first security data, the key data for use in decoding stored encoded data;

providing at least one biometric information sample; and

securing the first security data in dependence upon at least one of the at least one biometric information sample.

14. A method of securing data as defined in claim 13, wherein the step of providing a first information sample to a computer system comprises the step of:

hashing the first information sample to produce a first hash value.

15. A method of securing data as defined in claim 13, comprising the steps of:

providing a second other information sample to the computer system;

hashing the second information sample to produce a second hash value;

encoding the key data in dependence upon the second hash value to produce second security data; and

securing the second security data in dependence upon at least one of the at least one biometric information sample.

16. A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing a password.

17. A method of securing data according to claim 13, wherein the step of providing information to a computer system comprises the step of providing information stored on a smart card.

18. A method of securing data according to claim 13, wherein the key data is used for encrypting data.

19. A method of securing data comprising the steps of:

providing a first information sample to a computer system;

providing at least one biometric information sample;

encoding the at least one biometric information sample using the first information sample;

encoding key data in dependence upon encoded biometric sample to produce first security data, the key data for use in decoding stored encoded data; and

securing the first security data in dependence upon at least one of the at least one biometric information sample.

20. A method of securing data according to claim 19, comprises the steps of:

providing a first information sample to a computer system for decoding the encoded biometric sample; and

comparing the decoded biometric sample against stored templates associated with the biometric information source.

21. A method of securing data as defined in claim 19 wherein the step of providing a first information sample to a computer system comprises the step of:

hashing the first information sample to produce a first hash value.